

SDS IronSphere for z/OS

Automate z/OS STIG Compliance Through Continuous Security Monitoring

When your business needs to meet demanding federal regulations and industry standards, but you rely on manual processing for security scans and auditing, proving compliance can be an ongoing chore of enormous time and effort.

IronSphere is your solution to continuously monitor the mainframe, automate security checks, and initiate reporting – and then help simplify auditing to prove compliance. What could take months to examine manually, IronSphere can automate in a few minutes, with low overhead and real-time results.

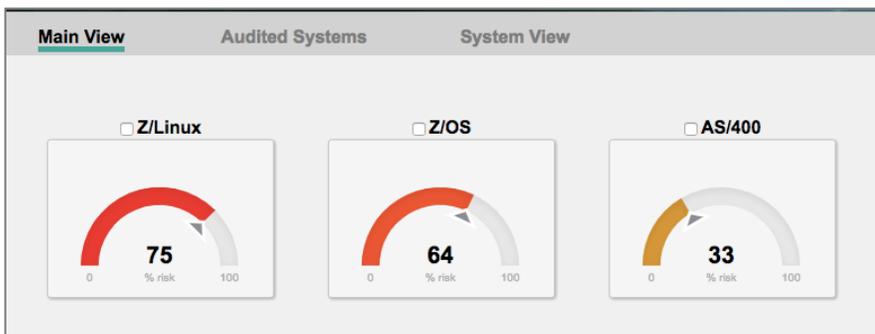
Security scans are based on DISA STIGs (Security Technical Information Guides from the Defense Information Systems Agency), which contain optimized policy and configuration information for system applications.

IronSphere automatically compares each application to its STIG to find system vulnerabilities, altered system settings, modified operands, and other discrepancies. If an issue is detected, IronSphere launches automatic diagnostic routines to determine:

- Security problems and errors
- Which components are affected
- Root cause of any problem
- Which issues are the highest risk

The resulting real-time report identifies errors, assigns risk levels, and charts the findings. It even describes how to resolve the problem.

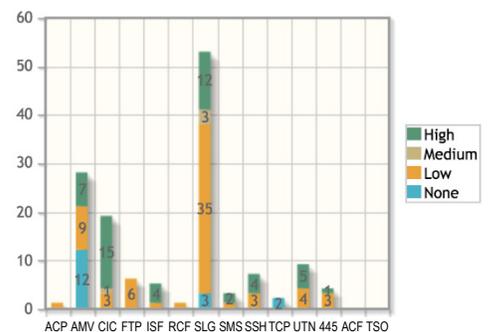
A dashboard reports the health of each system with intuitive, color-coded graphs.



Compliance, Continuous Monitoring, and Data Protection

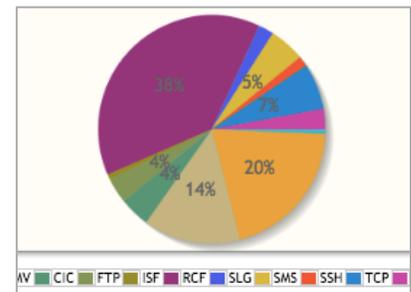
IronSphere helps comply with GDPR, NIST ISCM, and DoD requirements.

- Real-time vulnerability reporting.**
- Mainframe DISA STIG monitoring.**
- Risk resolution sent to your inbox.**
- Simplifies complicated mandates.**
- Easy z/OS security audits.**



Risk levels within each group.

Distribution of a risk level across groups.



Data is displayed graphically in easy-to-understand charts and tables. Results can be sorted and filtered per system, LPAR, group, severity level, or other criteria.

Simplify mainframe security! Intuitive IronSphere GUI gives you the problem resolution.



Name	Severity	Issue
MVS-AMV-040-00	Low	Inaccessible APF libraries defined.
MVS-AMV-160-00	Medium	Inapplicable PPT entries have not been removed.
MVS-AMV-325-00	None	Non-existent or inaccessible Link Pack Area (LPA) libraries.
MVS-AMV-350-00	None	Non-existent or inaccessible LINKLIST libraries.
MVS-AMV-410-00	None	z/OS UNIX OMVS parameters in PARMLIB are not properly specified.
MVS-AMV-440-00	None	Database is not on separate physical devices.
MVS-ACP-010-00	Medium	SWRDSWORD data set and OSpassword data set are not protected.
MVS-ACP-020-00	None	Access to SYS1 LINKLIB is not properly limited to only system programmers.
MVS-ACP-030-00	None	Write or greater access to SYS1 SYSPROC is not limited to only system programmers.
MVS-ACP-040-00	High	Write or greater access to SYS1 IMA is not limited to only system programmers.

Security and GRC teams are z/OS risk-aware: Automatic assessments detect changes in the status of system components, identify risk levels, and report all results from a single graphical interface. IronSphere can conclusively prove an application is error-free and in compliance with security standards.

IronSphere can validate that an application or group meets security standards and a log history can conclusively prove system integrity and continuous monitoring. Results are retained within the IronSphere server, allowing auditors easy access for compliance verification.

A dashboard reports the health of each system with graphs for any level of user, regardless of mainframe expertise. Results can be shown in a variety of comparison and history charts to suit the needs of any management or security team.

IronSphere helps satisfy the compliance requirements of: PCI, GDPR, 23 NYCRR 500, and more; SOX, GLBA, HIPAA.

Each IronSphere agent reports diagnostic results to the secure server over HTTPS. Messages and trace data are not stored on the mainframe.

Name	Severity	Issue
MVA-AMV-350-00	None	Non-existent or inaccessible LINKLIST libraries.
MVA-USS-011-00	None	z/OS UNIX OMVS parameters in PARMLIB are not properly specified.
MVA-ACP-070-00	None	Write or greater access to all LPA libraries must be limited to system programmers only.
MVA-AMV-325-00	None	Non-existent or inaccessible Link Pack Area (LPA) libraries.
MVA-ACP-010-00	None	SYS1.PARMLIB is not limited to only system programmers.

<p>Information</p> <table border="1"> <tr><td>Name</td><td>MV3A</td></tr> <tr><td>Type</td><td>z/OS 02.03.00 HBB77B0</td></tr> <tr><td>Class</td><td>Data Integrity</td></tr> <tr><td>Description</td><td>SYS1.PARMLIB contains the parameters which control system IPL, configuration characteristics, security facilities, and performance. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.</td></tr> <tr><td>Responsibility</td><td>Information Assurance Officer</td></tr> </table>	Name	MV3A	Type	z/OS 02.03.00 HBB77B0	Class	Data Integrity	Description	SYS1.PARMLIB contains the parameters which control system IPL, configuration characteristics, security facilities, and performance. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.	Responsibility	Information Assurance Officer	<p>Fix</p> <p>The IAO will ensure that update and alter access to SYS1.PARMLIB is limited to system programmers only and all update and alter access is logged. Review access authorization to critical system files. Evaluate the impact of correcting the deficiency. Develop a plan of action and implement the changes as required.</p> <p>The IAO will implement controls to specify the valid users authorized to update the SYS1.PARMLIB concatenation. All update and alter access to libraries in the concatenation will be logged using the ACP's facilities.</p> <p>1. That systems programming personnel will be authorized to update and alter the SYS1.PARMLIB concatenation. 2. That domain level security administrators can be authorized to update the SYS1.PARMLIB concatenation. 3. That System Level Started Tasks, authorized Data Center personnel, and auditor can be authorized read access by the IAO. 4. That all update and alter access is logged.</p>
Name	MV3A										
Type	z/OS 02.03.00 HBB77B0										
Class	Data Integrity										
Description	SYS1.PARMLIB contains the parameters which control system IPL, configuration characteristics, security facilities, and performance. Unauthorized access could result in the compromise of the operating system environment, ACP, and customer data.										
Responsibility	Information Assurance Officer										

Detailed STIG information is displayed in one location, including the fix.



For more information about SDS IronSphere for z/OS, please visit sdsusa.com/ironsphere.

Quality Mainframe Software Since 1982
 Software Diversified Services delivers comprehensive, affordable mainframe and distributed software with a focus on cybersecurity and compliance. Hundreds of organizations worldwide, including many Fortune 500 companies, rely on SDS software. Our expert development and award-winning technical support teams are based in Minneapolis, MN. To learn more, please visit our website.
 All non-SDS products may be trademarks of their respective companies.
 © Software Diversified Services